#4

jc997 U.S. PTO
10/057757
01/25/02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of	: **Makoto TANAKA, et al.**
Filed:	: **Concurrently herewith**
For:	: **INFORMATION STORAGE MEDIUM...**
Serial No.	: **Concurrently herewith**

Assistant Commissioner for Patents
Washington, D.C. 20231

January 25, 2002

PRIORITY CLAIM AND SUBMISSION

OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **JAPANESE** patent application no. **2001-017511** filed **January 25, 2001,** a certified copy of which is enclosed and application no. **2002-6280** filed on January 15, 2002, a certified copy will follow.

Any fee, due as a result of this paper, not covered by an enclosed check, may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,

Harris A. Wolin
Reg. No. 39,432

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.: SCES 19.360
TELEPHONE: (212) 940-8800

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２００１年 １月２５日

出 願 番 号
Application Number: 特願２００１－０１７５１１

出 願 人
Applicant(s): 株式会社ソニー・コンピュータエンタテインメント

２００１年 ９月１２日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　SCEI00082

【提出日】　平成13年 1月25日

【あて先】　特許庁長官殿

【国際特許分類】　G06K 19/00

【発明者】

【住所又は居所】　東京都港区赤坂７－１－１　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　田中　誠

【発明者】

【住所又は居所】　東京都港区赤坂７－１－１　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　犬井　努

【特許出願人】

【識別番号】　395015319

【氏名又は名称】　株式会社ソニー・コンピュータエンタテインメント

【代理人】

【識別番号】　100099324

【弁理士】

【氏名又は名称】　鈴木　正剛

【電話番号】　03-5441-4351

【選任した代理人】

【識別番号】　100108604

【弁理士】

【氏名又は名称】　村松　義人

【選任した代理人】

【識別番号】　100111615

【弁理士】

【氏名又は名称】　佐野　良太

【手数料の表示】

【予納台帳番号】　031738

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　記録媒体、情報処理装置、コンテンツ配信サーバ、方法、プログラム、記録媒体

【特許請求の範囲】

【請求項１】　管理情報を記録する第１記録領域と、暗号化された前記管理情報を記録する第２記録領域とを有する、記録媒体。

【請求項２】　記録媒体の第１記録領域に管理情報を書き込む工程と、前記記録媒体の第２記録領域に暗号化された前記管理情報を書き込む工程とを含む、記録媒体の製造方法。

【請求項３】　情報処理装置において実行される方法であって、検証対象となる記録媒体に記録された管理情報と暗号化された前記管理情報とを読み込む処理と、前記暗号化された管理情報を復号する処理と、前記読み込まれた管理情報と前記復号された管理情報とを比較する処理とを含み、前記比較の結果、前記読み込まれた管理情報と前記復号された管理情報とが所定の対応関係にあるときに検証対象の記録媒体が正当であると認定する方法。

【請求項４】　前記暗号化された管理情報は秘密鍵情報を利用した暗号技術により暗号化されており、前記復号する処理は当該秘密鍵情報により実行される、請求項３記載の方法。

【請求項５】

管理情報を記録する第１記録領域と暗号化された前記管理情報を記録する第２記録領域とを有する記録媒体の正当性を検証する情報処理装置であって、

前記記録媒体から前記管理番号および前記暗号化された管理番号を読み取るとともに、読み取った前記暗号化された管理番号の復号を制御する制御部と、

前記読み取った管理番号と前記復号された管理番号とが所定の対応関係にあるか否かを判定するとともに、その判定結果が肯定的なときに前記記録媒体が正当であると認定する比較部とを有する、情報処理装置。

【請求項６】　ネットワークを介して接続されたユーザ端末からの要求に応じて、コンテンツデータを前記ユーザ端末に送出するコンテンツ配信サーバにおいて実行されるユーザ端末の管理方法であって、

前記ユーザ端末の記憶装置に記録されている管理情報および暗号化された管理情報の送信を要求する処理と、

前記管理情報および暗号化された管理情報を受信する処理と、

受信した前記暗号化された管理情報を復号する処理と、

前記読み込まれた管理情報と前記復号された管理情報とが所定の対応関係にあるか否かを判定する判定処理と、

前記判定処理の結果が肯定的なときに前記管理情報が正当であると認定する処理と、

前記認定の結果が肯定的なときに、前記ユーザ端末からの要求に応じることを特徴とするユーザ端末の管理方法。

【請求項７】　前記認定された管理情報が所定の管理情報リストに含まれているか否かを判定する追加の判定処理をさらに含み、

前記追加の判定処理の結果が肯定的なときには、前記ユーザ端末からの要求に応じることを制限する、請求項６記載のユーザ端末の管理方法。

【請求項８】　前記所定の管理情報リストは、コンテンツデータファイルの送出を制限する対象となるユーザ端末の管理情報から構成される、請求項７記載のユーザ端末の管理方法。

【請求項９】　ネットワークを介して接続されたユーザ端末からの要求に応じて、コンテンツデータを前記ユーザ端末に送出するコンテンツ配信サーバであって、

前記ネットワークとの間でデータの入出力を行うインターフェイス部と、

前記インターフェイス部を介して、ユーザ端末の記憶媒体に記録されている管理情報および暗号化された管理情報の送信を要求するとともに、受信された前記暗号化された管理情報の復号を制御する制御部と、

前記受信された管理情報と前記復号された管理情報とが所定の対応関係にあるか否かを判定するとともに、その判定結果が肯定的なときに前記管理情報が正当であると認定する比較部とを有し、

前記制御部は、前記認定結果が否定的であるときに、前記ユーザ端末への前記コンテンツデータの送出を制限する、ことを特徴とするコンテンツ配信サーバ。

【請求項１０】　ネットワークを介して接続されたユーザ端末からの要求に応じて、コンテンツデータを前記ユーザ端末に送出するコンテンツ配信サーバであって、

前記ネットワークとの間でデータの入出力を行うインターフェイス部と、

前記インターフェイス部を介して、ユーザ端末の記憶媒体に記録されている管理情報および暗号化された管理情報の送信を要求するとともに、受信された前記暗号化された管理情報の復号を制御する制御部と、

前記受信された管理情報と前記復号された管理情報とが所定の対応関係にあるか否かを判定するとともに、その判定結果が肯定的なときに前記管理情報が正当であると認定する第１比較部と、

コンテンツデータファイルの送出を制限する対象となる記録媒体の管理情報から構成される管理情報データベースと、

前記認定された管理情報が所定の前記管理情報データベースに含まれているか否かを判定する第２比較部とを含み、

前記制御部は、前記第１比較部による認定結果が肯定的であり、かつ前記第２比較部による判定結果が否定的であるときに、前記ユーザ端末への前記コンテンツデータの送出を許可する、ことを特徴とするコンテンツ配信サーバ。

【請求項１１】　記録媒体の第１記録領域に管理情報を書き込む処理と、前記記録媒体の第２記録領域に暗号化された前記管理情報を書き込む処理とを情報処理装置に実行させるコンピュータプログラム。

【請求項１２】　検証対象となる記録媒体に記録された管理情報と暗号化された前記管理情報とを読み込む処理と、前記暗号化された管理情報を復号する処理と、前記読み込まれた管理情報と前記復号された管理情報とを比較する処理と、前記比較の結果、前記読み込まれた管理情報と前記復号された管理情報とが所定の対応関係にあるときに検証対象の記録媒体が正当であると認定する処理とを、情報処理装置に実行させるコンピュータ・プログラム。

【請求項１３】　ネットワークを介して接続されたユーザ端末からの要求に応じて、コンテンツデータを前記ユーザ端末に送出するコンテンツ配信サーバに

前記ユーザ端末の記憶装置に記録されている管理情報および暗号化された管理情報の送信を要求する処理と、

前記管理情報および暗号化された管理情報を受信する処理と、

受信した前記暗号化された管理情報を復号する処理と、

前記読み込まれた管理情報と前記復号された管理情報とが所定の対応関係にあるか否かを判定する判定処理と、

前記判定処理の結果が肯定的なときに前記管理情報が正当であると認定する処理とを実行させ、

前記認定処理の結果が否定的なときに、前記ユーザ端末からの要求に応じる処理の実行を制限させるコンピュータプログラム。

【請求項１４】　請求項１１、１２または１３に記載されたコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【発明の属する技術分野】　本発明はデータ記録媒体の管理技術、およびこの管理技術を応用したコンテンツ配信システムに関する。

【従来技術】　ハードディスク装置に代表される情報の記録装置または媒体（以下、本明細書においては、両者を単に記録媒体と呼ぶ。）に管理情報を記録することは、従来からよく行われている。

図１は、そのような管理情報の一種であるシリアル番号の例を示す図である。この例においては、シリアル番号は、全体１６バイトの長さを有し、それぞれ意味の異なる情報を示す複数のコードから構成される。このシリアル番号の例においては、図中左から右に、メーカーコードに２バイト、製造工場コードに２バイト、製品コードに４バイト、ロット番号に４バイト、連続番号に４バイトが割り当てられている。メーカーコードとは、その記録媒体を製造したメーカーを識別するための情報であって、メーカー毎に一意なコードが割り当てられる。製造工場コードとは、その記録媒体を製造した工場を識別するための情報であって、工場毎に一意なコードが割り当てられる。製品コードとは、その記録媒体の種類、製品番号、バージョン番号等を識別するための情報であって、製品毎に一意なコードが割り当てられる。ロット番号とは、製造ロット（製造単位）を識別するた

めの情報であって、製造ロット毎に一意なコードが割り当てられる。連続番号とは、その記録媒体を識別するための情報であって、同一製造ロットにおいて一意な番号が割り当てられる。

このような管理情報の記録は、主に記録媒体の品質管理を目的として行われている。すなわち、記録媒体に品質上の問題が発生した場合に、そのシリアル番号を参照すれば、その記録媒体がどのメーカーの、どの工場で、どの製造ロットで生産したものかを特定することにより、事後処理に役立てることができる。

このような管理情報は、従来、記録媒体の生産工程において、記録媒体の通常の記録領域に、通常の符号形式を用いて書き込まれる。ここで通常の記憶領域とは、ユーザが一般的な情報処理装置および記録媒体の読み書き装置（パーソナルコンピュータ、ドライブ類）を用いて読み書きできる記録媒体の領域を指す（いわゆる管理領域を含む）。通常の符号とは、上記読み書き装置によって解読可能な一般的な符号（ASCII符号、JIS符号等）を指す。

【解決すべき課題】

一方、上述のように、従来管理情報は、記録媒体にユーザが読み書き可能な形式で記録されているため、ユーザが管理情報を参照して、これを改ざんすることも可能である。ユーザによる管理情報の改ざんを防止するためには管理情報を、（１）通常の手段では（一般的な読み書き装置では）書き込みできない記録領域に書き込む、または（２）一度書き込むと書き換え不可能なデバイス（ROM等）に書き込む、ことが考えられる。

しかしながら、上記（１）の方法ではユーザに書き込み手段を発見されると改ざんが可能になってしまうため、一度書き込み手段を発見されるとすべての記録媒体の管理情報を信頼できなくなってしまう。

また、上記（２）の手段では改ざんは困難になるが、ROM等のデバイスを追加することにより記録媒体の生産コストが高くなるうえに、デバイスごと交換されてしまうおそれがある。

管理情報の改ざんが簡単に行われるような状況では、上述した管理情報を利用した品質管理は実現困難になる。

また、最近では、記録媒体に記録された管理情報を利用して、顧客の管理を行

おうとする試みがある。このような場合でも、管理情報の改ざんが簡単に行われると、管理情報を利用した顧客管理は実現困難になる。

したがって、本発明の目的の一つは、記録媒体の管理情報の改ざんを確実に検出するとともに、その正当性を確実に検証するための技術を提供することにある。

また、本発明の他の目的は、記録媒体の管理情報の改ざんを確実に検出することができ、その正当性を確実に検証できる記録媒体、そのための方法、装置を提供することにある。

さらに、本発明の他の目的は、上記記録媒体の管理情報の改ざんの検出および正当性の検証技術を応用したコンテンツ配信システム、コンテンツ配信方法を提供することにある。

さらに、本発明の他の目的は、上記の方法を情報処理装置に実行させるコンピュータ・プログラムおよびプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

【課題を解決するための手段】

上記課題に対応した、本発明の記録媒体は、管理情報を記録する第１記録領域と、暗号化された前記管理情報を記録する第２記録領域とを有する、ことを特徴とする。本発明の「記録媒体」とは、ハードディスク装置、フレキシブルディスク、追記可能なＣＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、磁気テープ、光磁気ディスク、バッテリバックアップ機能付きのＲＡＭメモリカートリッジ、フラッシュメモリ（商標）カートリッジ、その他の不揮発性メモリカートリッジ等の追記可能な記録領域を有するすべての情報記録媒体を包含する概念である。また、本発明の「管理情報」とは、ある記録媒体を他の記録媒体から区別するために付与される情報であって、代表的な例としてはシリアル番号がある。

この記録媒体は、その適切な記録領域（第３、第４、．．．．、第ｎ記録領域）に暗号化された前記管理情報がさらに記録されたものでもよい。このような追加的に記録される暗号化された管理情報は、第２記録領域に記録された暗号化された管理情報とは、別の暗号鍵を用いて暗号化したものでもよいし、別の暗号技術を用いて暗号化したものでもよい。

上記課題に対応した、本発明の記録媒体の製造方法は、記録媒体の第１記録領域に管理情報を書き込む工程と、前記記録媒体の第２記録領域に暗号化された前記管理情報を書き込む工程とを含む、ことを特徴とする。

この記録媒体の製造方法においては、追加的な記録領域（第３、第４、．．．、第ｎ記録領域）に暗号化された管理情報をさらに記録することも可能である。このような追加的な暗号化された管理情報の記録は、第２記録領域に記録された暗号化された管理情報とは、別の暗号鍵を用いて暗号化したものでもよいし、別の暗号技術を用いて暗号化したものでもよい。

上記課題に対応した本発明の記録媒体の正当性を検証するための方法は、情報処理装置において実行される方法であって、検証対象となる記録媒体に記録された管理情報と暗号化された前記管理情報とを読み込む処理と、前記暗号化された管理情報を復号する処理と、前記読み込まれた管理情報と前記復号された管理情報とを比較する処理とを含み、前記比較の結果、前記読み込まれた管理情報と前記復号された管理情報とが所定の対応関係にあるときに検証対象の記録媒体が正当であると認定することを特徴とする。ここで、所定の対応関係とは、読み込まれた管理情報と復号された管理情報とが完全に一致する場合、それらの一部分が一致する場合、その他一定の法則性に従って対応付けが可能な関係すべてを含むものである（以下、この項において同じ。）。

この正当性検証方法において、管理情報を秘密鍵情報を利用した暗号技術により暗号化し、復号する処理は当該秘密鍵情報により実行することができる。

記録媒体に2以上の暗号化された管理情報が記録されている場合には、上記の読み込む処理においてそれらの暗号化された管理情報をすべて読み込み、暗号化された管理情報をすべて復号処理し、読み込まれた管理情報と復号された２以上の管理情報とがすべて所定の対応関係にある場合にのみ、検証対象の記録媒体が正当であると認定することも可能である。

上記課題に対応した本発明の記録媒体の正当性検証装置は、管理情報を記録する第１記録領域と暗号化された前記管理情報を記録する第２記録領域とを有する記録媒体の正当性を検証する情報処理装置であって前記記録媒体から前記管理番号および前記暗号化された管理番号を読み取るとともに、読み取った前記暗号化さ

れた管理番号の復号を制御する制御部と、前記読み取った管理番号と前記復号された管理番号とが所定の対応関係にあるか否かを判定するとともに、その判定結果が肯定的なときに前記記録媒体が正当であると認定する比較部とを有する、ことを特徴とする。ここで、暗号化された管理番号の復号は、制御部の制御に従い、復号部で行うことができる。

記録媒体に2以上の暗号化された管理情報が記録されている場合には、この正当性検証装置が、記録媒体からそれらの暗号化された管理情報をすべて読み込み、暗号化された管理情報をすべて復号処理し、読み込まれた管理情報と復号された２以上の管理情報とがすべて所定の対応関係にある場合にのみ、検証対象の記録媒体が正当であると認定するようにしてもよい。

さらに、記録媒体に、異なった暗号化技術を用いて２以上の暗号化された管理情報が記録されている場合には、この正当性検証装置の制御部はそれらの暗号化技術に対応した復号機能を備えるようにして、それら暗号化された管理情報をすべて復号処理し、読み込まれた管理情報と復号された２以上の管理情報とがすべて所定の対応関係にある場合にのみ、検証対象の記録媒体が正当であると認定するようにしてもよい。

上記課題に対応した本発明のコンテンツ配信方法は、ネットワークを介して接続されたユーザ端末からの要求に応じて、コンテンツデータを前記ユーザ端末に送出するコンテンツ配信サーバにおいて実行されるユーザ端末の管理方法であって、前記ユーザ端末の記憶装置に記録されている管理情報および暗号化された管理情報の送信を要求する処理と、前記管理情報および暗号化された管理情報を受信する処理と、受信した前記暗号化された管理情報を復号する処理と、前記読み込まれた管理情報と前記復号された管理情報とが所定の対応関係にあるか否かを判定する判定処理と、前記判定処理の結果が肯定的なときに前記管理情報が正当であると認定する処理と、前記認定の結果が肯定的なときに、前記ユーザ端末からの要求に応じることを特徴とする。ここで、前記管理情報が正当であるとの認定はユーザ端末からの要求に応じるための前提条件であって、ユーザ端末からの要求の内容に応じてその他の付加的な要件を課すことを排除するものではない。また、「前記認定の結果が肯定的なときに、前記ユーザ端末からの要求に応じる

」かわりに、前記認定の結果が否定的なときに、前記ユーザ端末へのコンテンツデータの送出を制限することとしてもよい。

上記コンテンツ配信サーバにおいて実行されるユーザ端末の管理方法において、前記認定された管理情報が所定の管理情報リストに含まれているか否かを判定する追加の判定処理をさらに行い、前記追加の判定処理の結果が肯定的なときには、前記ユーザ端末からの要求に応じることを制限してもよい。

また、前記所定の管理情報リストを、コンテンツデータファイルの送出を制限する対象となるユーザ端末の記録媒体の管理情報のリストとすることにより、特定のユーザに対するコンテンツデータの配信を制限することができる。

上記課題に対応した本発明のコンテンツ配信サーバは、ネットワークを介して接続されたユーザ端末からの要求に応じて、コンテンツデータを前記ユーザ端末に送出するコンテンツ配信サーバであって、前記ネットワークとの間でデータの入出力を行うインターフェイス部と、前記インターフェイス部を介して、ユーザ端末の記憶媒体に記録されている管理情報および暗号化された管理情報の送信を要求するとともに、受信された前記暗号化された管理情報の復号を制御する制御部と、前記受信された管理情報と前記復号された管理情報とが所定の対応関係にあるか否かを判定するとともに、その判定結果が肯定的なときに前記管理情報が正当であると認定する比較部とを有し、前記制御部は、前記認定結果が否定的であるときに、前記ユーザ端末への前記コンテンツデータの送出を制限する、ことを特徴とする。

上記課題に対応した本発明の別のコンテンツ配信サーバは、ネットワークを介して接続されたユーザ端末からの要求に応じて、コンテンツデータを前記ユーザ端末に送出するコンテンツ配信サーバであって、前記ネットワークとの間でデータの入出力を行うインターフェイス部と、前記インターフェイス部を介して、ユーザ端末の記憶媒体に記録されている管理情報および暗号化された管理情報の送信を要求するとともに、受信された前記暗号化された管理情報の復号を制御する制御部と、前記受信された管理情報と前記復号された管理情報とが所定の対応関係にあるか否かを判定するとともに、その判定結果が肯定的なときに前記管理情報が正当であると認定する第１比較部と、コンテンツデータファイルの送出を制

限する対象となる記録媒体の管理情報から構成される管理情報データベースと、

前記認定された管理情報が所定の前記管理情報データベースに含まれているか否かを判定する第２比較部とを含み、前記制御部は、前記第１比較部による認定結果が肯定的であり、かつ前記第２比較部による判定結果が否定的であるときに、前記ユーザ端末への前記コンテンツデータの送出を許可する、ことを特徴とする。

ここで、第１比較部による認定結果が肯定的であること、および第２比較部による判定結果が否定的であることは、ユーザ端末へのコンテンツデータの送出を許可するための前提条件であって、ユーザ端末からの要求の内容に応じてその他の付加的な要件を課すことを排除するものではない。

上記課題に対応した本発明のプログラムは、上記記録媒体の製造方法を情報処理装置に実行させることを特徴とする。

上記課題に対応した本発明の別のプログラムは、検証対象となる記録媒体に記録された管理情報と暗号化された前記管理情報とを読み込む処理と、前記暗号化された管理情報を復号する処理と、前記読み込まれた管理情報と前記復号された管理情報とを比較する処理と、前記比較の結果、前記読み込まれた管理情報と前記復号された管理情報とが所定の対応関係にあるときに検証対象の記録媒体が正当であると認定する処理とを、情報処理装置に実行させることを特徴とする。

上記課題に対応した本発明のさらに別のプログラムは、ネットワークを介して接続されたユーザ端末からの要求に応じて、コンテンツデータを前記ユーザ端末に送出するコンテンツ配信サーバに、前記ユーザ端末の記憶装置に記録されている管理情報および暗号化された管理情報の送信を要求する処理と、前記管理情報および暗号化された管理情報を受信する処理と、受信した前記暗号化された管理情報を復号する処理と、前記読み込まれた管理情報と前記復号された管理情報とが所定の対応関係にあるか否かを判定する判定処理と、前記判定処理の結果が肯定的なときに前記管理情報が正当であると認定する処理とを実行させ、前記認定処理の結果が否定的なときに、前記ユーザ端末からの要求に応じる処理の実行を制限させることを特徴とする。

上記課題に対応した本発明のコンピュータプログラムを記録した記録媒体は、

上記のコンピュータプログラムを記録してなることを特徴とする。

【発明の実施の形態】

以下、図面を参照して本発明の一実施形態について説明する。

図２は、本発明の一実施形態をブロック図で示したものである。図２において、１０は記録媒体であり、２０は記録媒体に記録された情報を読み書きするための情報処理装置である。

まず、記録媒体１０について説明する。記録媒体１０は、第１記録領域１１、第２記録領域１２、第３記憶領域１３、入出力部１４を含んで構成される。第１記録領域には、この記録媒体の管理情報であるシリアル番号が記録される。シリアル番号は上述の図１に記載されたような情報を含むものでよいが、それに限定されるものでなく、記録媒体１０を一意に特定するのに十分な情報（番号、符号、記号またはそれらの組み合わせを含む）であればよい。第２記録領域には、暗号化されたシリアル番号が記録される。第３領域には、一般的な情報（プログラム、イメージデータ、音楽データ等）が記録される。

次に情報処理装置２０について説明する。情報処理装置２０は、記録媒体に付与するシリアル番号を記憶するシリアル番号記憶部２１と、暗号化・復号処理に用いられる暗号鍵を記憶する暗号鍵記憶部２２と、シリアル番号を暗号鍵を用いて暗号化する暗号化部２３と、暗号化されたシリアル番号を暗号鍵を用いて復号する復号部２４と、復号されたシリアル番号と記録媒体から読み込まれた暗号化されていないシリアル番号とを比較する比較部２５と、情報処理装置２０全体の動作を制御する制御部２６とを含んで構成される。ここで、比較部２５は、復号部２４によって復号されたシリアル番号と、記録媒体から読み込まれた暗号化されていないシリアル番号とを比較して、両者が一致しているか否かを判定する。制御部２６は、上記各機能部の動作を制御する（図面中各機能部への接続線は、比較部２５、記録媒体１０へのものを除き省略した）。

上記各機能部２１－２６は、情報処理装置がハードディスク装置または半導体メモリ等に記録されているコンピュータプログラム、データ等を読み込んで、コンピュータが搭載している基本制御プログラム（オペレーティング・システム）と協働することによって形成することができる。

＜実施形態の動作＞

次に、上記構成を有する記録媒体と情報処理装置の動作を説明する。

＜書き込み動作＞

まず、記録媒体１０への、シリアル番号および暗号化されたシリアル番号の書き込み動作について説明する。記録媒体１０を情報処理装置２０に接続し、情報処理装置２０に接続された外部入力装置（図示せず）を介してシリアル番号の書き込みを指示する。情報処理装置２０は、外部入力装置からの指示に従い適切なシリアル番号をシリアル番号記憶部２１から選択し、そのシリアル番号を記録媒体１０の第１記録領域に書き込む。また、情報処理装置は暗号鍵記憶部２２から暗号鍵を読み出し、暗号化部２３において上記選択されたシリアル番号を暗号化する。続いて、情報処理装置２０は、この暗号化されたシリアル番号を記録媒体の第２記録領域に書き込む。

ここで、暗号化部２３における暗号化は既知の暗号化技術（たとえば、共通鍵暗号方式）を用いて行うことができる。共通鍵暗号化方式には、DES(Data Encryption Standard)、Triple-DES、MARS、RC6等がある。ただし、本発明における暗号化技術は、共通鍵暗号化方式に限定されるものではなく、公開鍵暗号化方式も利用可能である。

必要に応じて、制御部２６により、情報処理装置２０に接続された情報記録装置（図示せず）から、記録媒体１０の第３記録領域にプログラム、イメージデータ、音楽データ等を書き込むことができる。

＜検証動作＞

次に、図３を参照して、シリアル番号および暗号化されたシリアル番号が書き込まれた記録媒体１０の正当性を検証するための動作について説明する。上記書き込み処理が行われた記録媒体１０を情報処理装置２０に接続すると、情報処理装置２０は、第１記憶領域から暗号化されていないシリアル番号、第２記録領域から暗号化されたシリアル番号を読み出す（ステップＳ１）。そして復号部２４は、第2記憶領域から読み出した暗号化されたシリアル番号を暗号鍵記憶部２２から取得した暗号鍵で復号する（ステップＳ２）。次に、比較部２５が復号されたシリアル番号と、記録媒体の第１記録領域から読み込まれたシリアル番号とを

比較し（ステップＳ３）、両者が一致しているか否かを判定する（ステップＳ４）。

ここで、記録媒体１０が正当なものであれば（例えば、シリアル番号の改ざんが行われていなければ）、比較部２５によって復号されたシリアル番号と、記録媒体の第１記録領域から読み込まれたシリアル番号とが一致するはずである。

そこで、判定結果が肯定的であるばあいには（ステップＳ４：YES）、正当な記録媒体であることを検証できたとして（ステップＳ５）、制御部２６は記録媒体１０の第３記録部との間での情報の読み書きを実行する。一方、判定結果が否定的であるばあいには（ステップＳ４：NO）、正当な記録媒体であることを検証できないとして（Ｓ６）、第３記録部との間での情報の読み書きを禁止または制限する。

以上説明したように、上記上記構成を有する記録媒体と情報処理装置によって、シリアル番号の改ざんを検出することができ、記録媒体の正当性を検証することができる。

＜応用実施例＞

＜コンテンツ・サーバ＞

インターネットに代表されるコンピュータネットワークの発達に伴ない、コンピュータプログラムや、電子書籍、音楽データ、動画データ等のいわゆるコンテンツをネットワーク経由で配信すること（コンテンツ配信サービス）が行われている。このようなコンテンツ配信サービスは、不特定多数のユーザに対して無料で行われているものも多いが、ネットワーク商取引が本格化するにつれ、特定の会員向けに有料で行われるもの（ネットワーク経由のコンテンツ販売）も増えると考えられる。

ネットワーク経由のコンテンツ販売は流通コストを最小限化できる反面、ひとたびネットワーク経由で流出した情報はその後の流通を適切に制限することが非常に困難である。例えば、ネットワーク上でコンテンツを購入したユーザがそれを第３者に無許可でコピーして配布したり、ネットワーク経由で配信したりすることが考えられる。コンテンツが汎用的なデータ形式（例えば、音楽データについてはMP3形式、電子書籍についてはPDF形式）で作成される限り、このような不

正なコピーの防止は困難である。特殊なデータ形式でコンテンツを作成し、専用の再生ソフトウェアの配布を厳格に管理することにより不正コピーをある程度制限可能であるが、サービスの汎用性および技術の進歩の速度を考慮するとそのようなデータ形式の採用は現実的ではない。

よって、コンテンツの配信者がコンテンツの流通を制御し、不正なコンテンツの利用をしたユーザに対してコンテンツの配信を制限できるような技術が求められている。

予めシリアル番号および暗号化されたシリアル番号を記録した記録媒体１０を会員登録したユーザに配布し、それらユーザのみを対象としてコンテンツの配信を行う、コンテンツ配信システムおよびコンテンツ配信サーバを実現することが考えられる。

以下、図面を参照して、このコンテンツ配信システムおよびコンテンツ配信サーバについて説明する。ここで、コンテンツ配信システムとは、電子書籍、音楽、映画、コンピュータソフトウェア等のコンテンツをネットワーク経由でユーザ端末に配信するサービスを実行するシステムをいう。コンテンツ配信サーバとは、コンテンツを記憶したデータベースを有し、ユーザからの要求に応じてコンテンツをユーザ端末に送信するサーバをいう（詳細な構成は以下で説明する）。

図４は、本実施例に係るコンテンツ配信システムの構成を示した概略図である。

本実施例のコンテンツ配信システムは、コンテンツ配信サーバ１００、ネットワークＬ、ユーザ端末１１０とから構成される。ネットワークＬはインターネット等のネットワークであり、コンテンツ配信サーバ１００と、ユーザ端末１１０とはネットワークＬを介して相互に接続される。

まず、コンテンツ配信サーバ１００について説明する。コンテンツ配信サーバ１００は、コンテンツ配信サーバ１００全体の機能・動作を制御する制御部１０１と、比較部１０２と、復号部１０３と、暗号鍵データベース（以下、データベースの語は、DBと省略する。）１０４と、コンテンツを記憶するコンテンツDB１０５と、会員管理のためのデータを記憶する会員管理DB１０６と、ネットワークLを介してユーザ端末１１０とのデータの送受信を行うためのネットワーク・イ

ンターフェイス（Ｉ／Ｆ）１０７とを含んで構成される。上記コンテンツ配信サーバ１００の各機能部１０１－１０６は、通信機能を有する情報処理装置がハードディスク装置または半導体メモリ等に記録されているコンピュータプログラム、データ等を読み込んで、コンピュータが搭載している基本制御プログラム（オペレーティング・システム）と協働することによって形成される。

ここで、比較部１０２は、上記実施形態中の情報処理装置２０における比較部２５に対応し、同様の機能を有する。また、復号部１０３は、上記実施形態中の情報処理装置２０における復号部２４に対応し、同様の機能を有する。さらに、暗号鍵DB１０４は、上記実施形態中の情報処理装置２０における暗号鍵記憶部２２に対応し、シリアル番号に対応した暗号鍵を記憶する。

次に、ユーザ端末１１０について説明する。ユーザ端末１１０は、ユーザ端末１１０全体の機能・動作を制御する制御部１１１と、記録媒体１０を接続するための記録媒体インターフェイス１１２と、ネットワークLを介してコンテンツ・サーバ１００とのデータの送受信を行うためのネットワーク・インターフェイス（Ｉ／Ｆ）１１３とを含んで構成される。ユーザ端末１１０は、ネットワーク通信機能を有し、ネットワークを介して記録媒体１０の読み書きが可能なパーソナルコンピュータ、ゲーム装置、エンターテインメント装置等でよい。

続いて、上記構成を有するコンテンツ配信システムの動作を説明する。

ユーザがユーザ端末１１０を介して、コンテンツ配信サーバ１００にアクセスすると、コンテンツ配信サーバ１００はネットワークを介して、ユーザ端末２０に接続された記録媒体の第１記憶領域から暗号化されていないシリアル番号、第２記録領域から暗号化されたシリアル番号を読み出す。そして復号部１０３は、第２記憶領域から読み出した暗号化されたシリアル番号を暗号鍵DB１０４から取得した暗号鍵で復号する。次に、比較部１０２が復号されたシリアル番号と、記録媒体の第１記録領域から読み込まれたシリアル番号とを比較し、両者が一致しているか否かを判定する。

ここで、記録媒体１０が正規会員に対して配布された正当なものであれば、比較部１０２によって復号されたシリアル番号と、記録媒体の第１記録領域から読み込まれたシリアル番号とが一致するはずである。

そこで、判定結果が肯定的である場合には、正当な会員であることを検証できたとして、制御部１０１はユーザからの要求に応じて、コンテンツDB１０５に記憶されたコンテンツをダウンロードすることを許可する。このとき、送出するコンテンツにそのユーザを特定するための情報（例：記録媒体のシリアル番号）を挿入しておいてもよい。ユーザ特定情報の挿入には、いわゆる電子透かし技術（例えば、IBM社が提供するData Hiding（商標））等を用いることが望ましいが、通常のデータの形式で挿入してもよい。このユーザ特定情報の利用方法については後述する。

一方、判定結果が否定的である場合には、正当な会員であることを検証できないとして、コンテンツDB１０５に記憶されたコンテンツをダウンロードすることを禁止または制限する。

このように、上記構成を有するコンテンツ配信システムによって、正当な会員のみに、コンテンツ配信サービスを提供することができる。第３者が正規会員の持つ記録媒体のシリアル番号を入手したとしても、それだけではコンテンツ配信サービスを利用することはできないことが理解されよう。

ところで、正規会員がダウンロードしたコンテンツを無許可で第３者にコピーしたり、インターネットウェブサイトにおいて公開したりすることが考えられる。コンテンツにユーザ特定情報を挿入しておくことにより、このようなコンテンツの不正使用を行ったユーザを特定することができる。

具体的には、コンテンツ配信システムの管理者が不法にコピーまたは公開されたコンテンツを発見した際に、それらのコンテンツからユーザ特定情報を取り出す。ユーザ特定情報からそのコンテンツをダウンロードした会員を特定し、そのような会員については以後のコンテンツ利用を禁止または制限するために、コンテンツ配信サーバ１００の管理者は会員管理DB１０６にコンテンツの配信を制限するための情報を記録する。例えば、会員管理DB１０６にブラックリストとして、利用を禁止する会員の所有する記録媒体のシリアル番号を記録しておく。コンテンツ配信サーバ１００は、比較部１０２における判定結果が肯定的である場合に、制御部１０１が会員管理DB１０６のブラックリストを参照して、判定したシリアル番号が含まれているか否かをチェックする。チェックの結果、ブラックリ

ストに判定したシリアル番号が記録されていれば、コンテンツDB１０５に記憶されたコンテンツをダウンロードすることを禁止または制限する。ブラックリストに記録されていなければ、ユーザからの要求に応じて、コンテンツDB１０５に記憶されたコンテンツをダウンロードすることを許可する。

従って、正規の会員がコンテンツの違法な利用を行った場合に、そのような会員に対して一定の制裁措置を与えることが可能になる。

以上、本発明を特定の実施形態および実施例（以下、実施形態等）に従って説明したが、本発明は上記実施形態等に限定されるものではない。例えば、上記実施形態等では、記録媒体から読み込んだ暗号化されたシリアル番号を情報処理装置内で復号して、復号されたシリアル番号を、暗号化されていないシリアル番号と比較しているが、逆に情報処理装置内で、記録媒体から読み取った暗号化されていないシリアル番号を暗号化して、これを暗号化されたシリアル番号と比較してもよい。つまり、記録媒体にセットで記録された暗号化されたシリアル番号と、暗号化されていないシリアル番号とが所定の相関関係を持つこと、通常は一致していること、を検証すれば十分である。

また、上記実施形態においては、記録媒体には暗号化されたシリアル番号は一つのみ記録したが、暗号化されたシリアル番号を２以上記録することとしてもよい。この際、シリアル番号を２つ以上の異なる暗号鍵で暗号化し、暗号化されたシリアル番号をそれぞれ、記録媒体の異なる記録領域上に記録する。記録媒体が正当なものであるかを検証するときは、それぞれの記録領域から暗号化されたシリアル番号を読み込んで対応する暗号鍵を用いて復号するとともに、暗号化されていないシリアル番号と比較を行えばよい。

さらに、シリアル番号を２つ以上の異なる暗号技術を用いて暗号化して、暗号化されたシリアル番号をそれぞれ記録媒体に記録することもできる。記録媒体が正当なものであるかを検証するときは、それぞれの記録領域から暗号化されたシリアル番号を読み込んで対応する暗号技術を用いて復号するとともに、暗号化されていないシリアル番号と比較を行えばよい。

２以上の暗号鍵を用いてシリアル番号を記録するためには、暗号鍵を予め必要な分だけ用意して、それぞれの暗号鍵でシリアル番号の暗号化を行うとともに、

生成された複数の暗号化されたシリアル番号を順に記録媒体の異なる記録領域に書き込めばよい。また、２以上の暗号技術を用いてシリアル番号を記録するためには、情報処理装置内にそれぞれの暗号技術に対応した暗号化部（暗号化機能）を用意して、シリアル番号をそれぞれの暗号化部で暗号化するとともに、生成された複数の暗号化されたシリアル番号を順に記録媒体の異なる記録領域に書き込めばよい。この記録媒体が正当なものであるかを検証するときは、それぞれの記録領域から暗号化されたシリアル番号を読み込んで、それぞれに対応する暗号技術を用いて復号するとともに、暗号化されていないシリアル番号と比較を行えばよい。この場合、一つの復号部が複数の暗号化技術に対応できるようにしてもよいし、それぞれの暗号化技術につき独立した復号部を設けるようにしてもよい。

このように複数の暗号鍵または暗号技術を用いることの利点として次のようなものがあげられる。

暗号化されたシリアル番号と暗号化されていないシリアル番号の両方を改ざんする可能性も考えられるが、複数の暗号鍵または暗号技術を解読または解析するためには技術的、時間的に困難である。したがって、シリアル復号された複数のシリアル番号と暗号化されていないシリアル番号のすべてが一致していれば、より高い確率で記録媒体の正当性を検証することができる。

また、暗号化されていないシリアル番号と暗号化されたシリアル番号のどちらも改ざんされる可能性があるため、復号したシリアル番号と暗号化されていないシリアル番号とが一致しない場合にはどちらかが（またはその両方が）改ざんされた事実はわかるが、どちらが正しいのかまたはその両方が正しくないのかは特定できない。このような場合でも、復号された複数のシリアル番号同士が一致していれば、それが正しいシリアル番号である確率が高いと推定される。したがって、正しいシリアル番号を特定し易くなる。

上記の記録媒体１０へのシリアル番号および暗号化されたシリアル番号の書き込み動作と、上記のシリアル番号および暗号化されたシリアル番号が書き込まれた記録媒体１０の正当性の検証動作は、情報処理装置（コンピュータ）に、本発明のコンピュータプログラムをコンピュータ読み取り可能な記録媒体から読み込ませて、それを実行させることにより実現可能になる。

上記のコンテンツ配信サーバは、通信機能を有するコンピュータに、本発明のコンピュータプログラムを実行させることによっても実現できる。

この場合、上記実施形態・実施例または図面に記載された各機能部は、コンピュータがアクセス（アクセスは記録・読み出しの意味）可能な記録媒体、例えばハードディスク装置または半導体メモリ、に記録されているコンピュータプログラム単体で、またはコンピュータが搭載している基本制御プログラム（オペレーティング・システム）との協働によって形成される。

【効果】　したがって、本発明により、記録媒体の管理情報の改ざんを確実に検出するとともに、その正当性を確実に検証することが可能になる。

また、本発明の記録媒体、そのための方法、装置により、記録媒体の管理情報の改ざんを確実に検出することができ、その正当性を確実に検証できる。

さらに、本発明のコンテンツ配信システムにより、コンテンツの配信者がコンテンツの流通を制御し、不正なコンテンツの利用をしたユーザに対してコンテンツの配信を制限できる。

【図面の簡単な説明】

【図1】　記録媒体に記録されるシリアル番号のデータ構造を示す図である。

【図2】　本発明の実施形態である記録媒体、情報処理装置を示すブロック図である。

【図3】　本発明の記録媒体の正当性を検証する方法を示す流れ図である。

【図４】　本発明の実施例であるコンテンツ配信システムを示すブロック図である。

【符号の説明】

１０　記録媒体

２０　情報処理装置

２１　シリアル番号記憶部

２２　暗号鍵記憶部

２３　暗号化部

２４　復号部

２５　比較部

２６　制御部

１００　コンテンツ配信サーバ

１０１　制御部

１０２　比較部

１０３　復号部

１０４　暗号鍵データベース

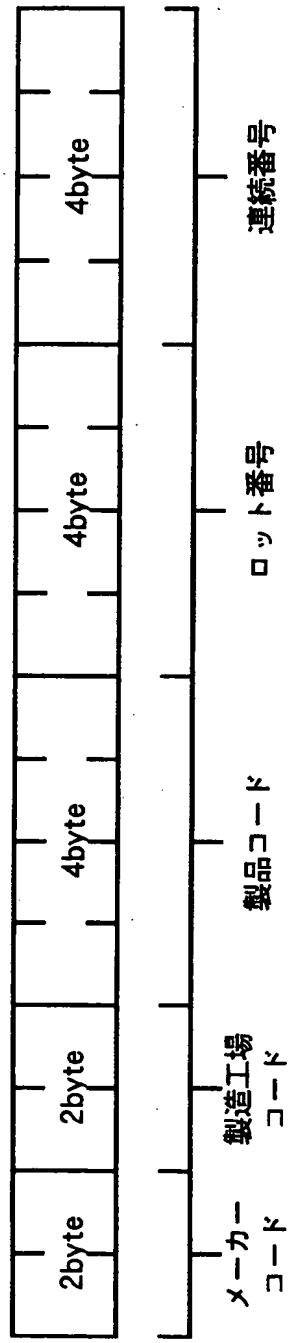
１０５　コンテンツデータベース

１０６　会員管理データベース

１１０　ユーザ端末

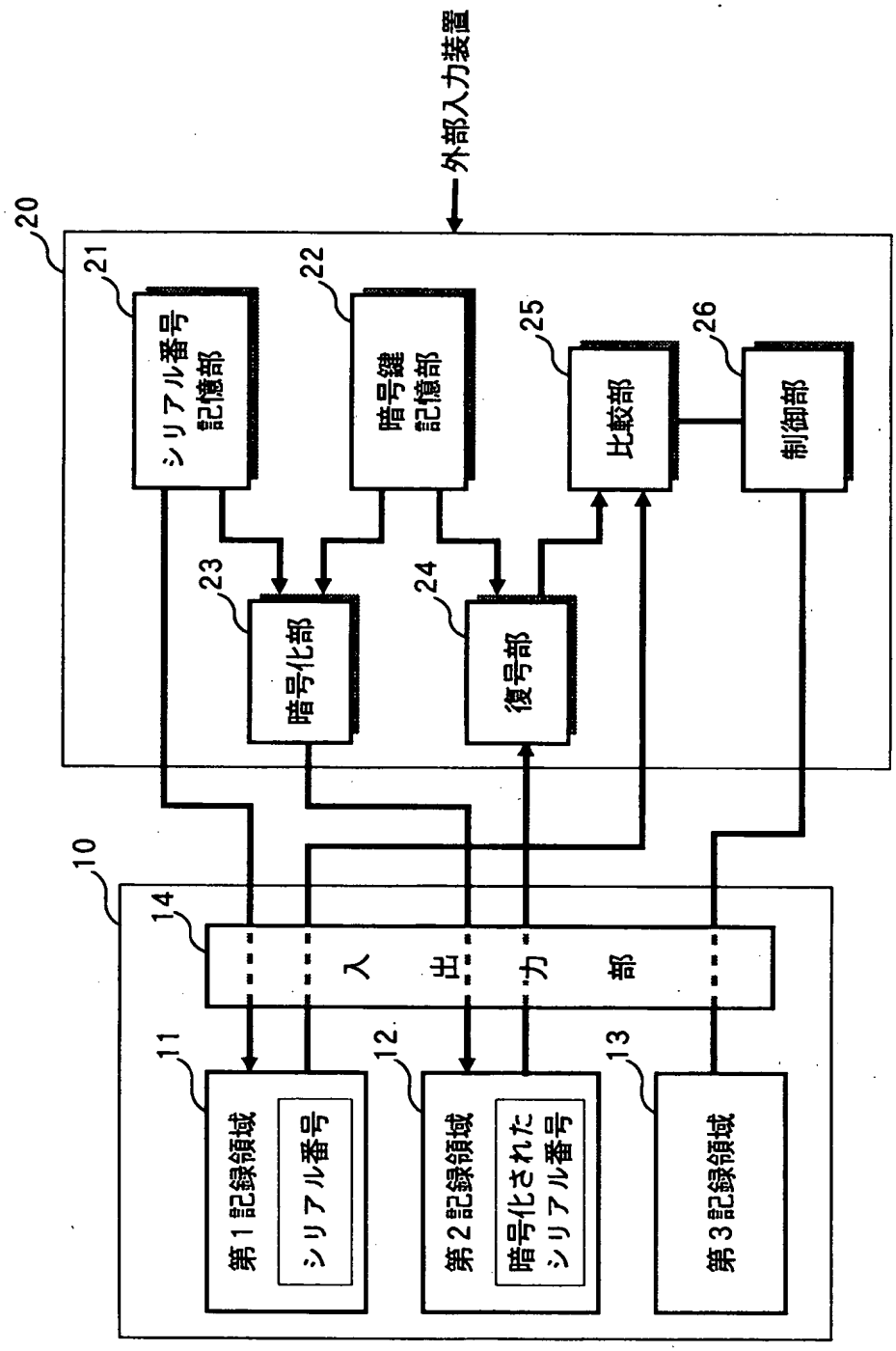
【書類名】　図面

【図１】

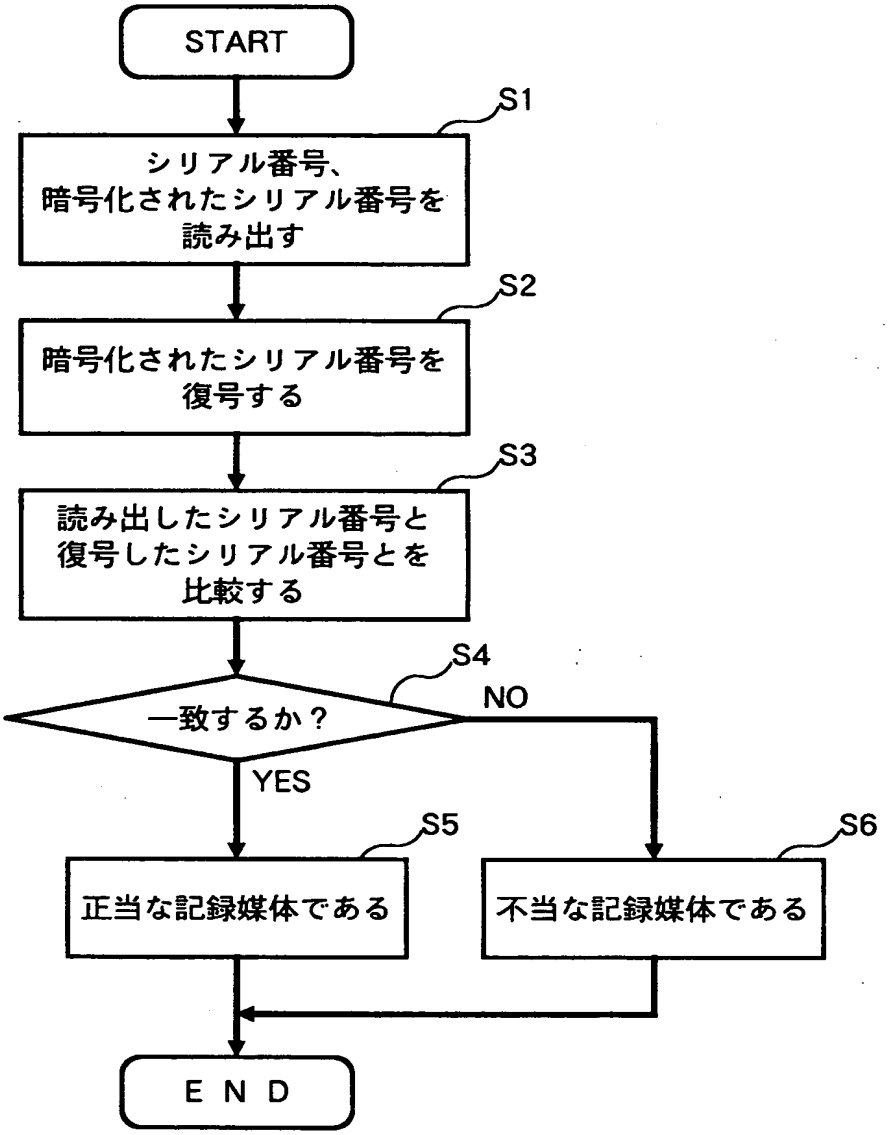


出証特２００１－３０８４２１３

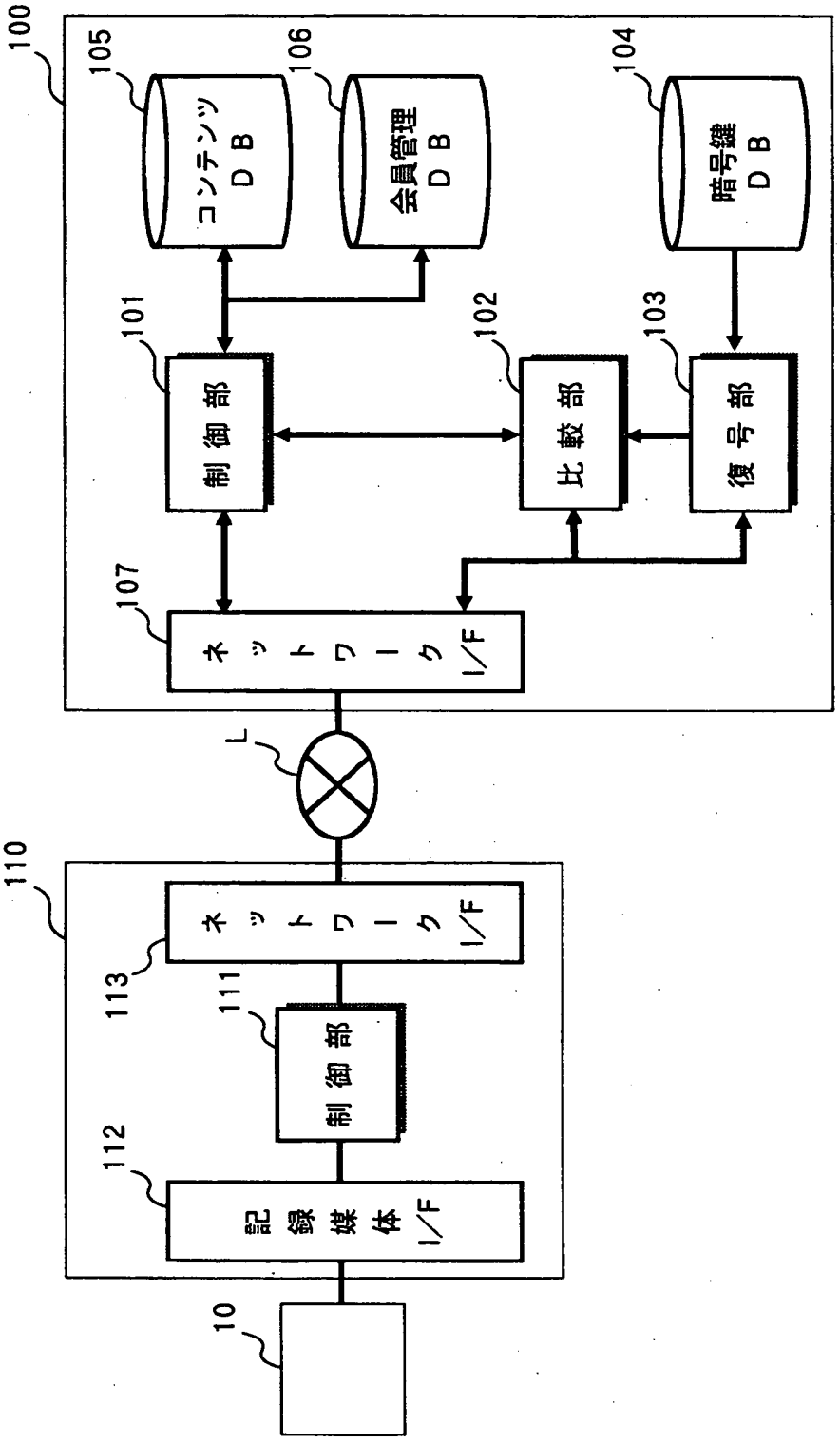
【図２】


外部入力装置
20
21
シリアル番号記憶部
22
暗号鍵記憶部
25
比較部
26
制御部
23
暗号化部
24
復号部
10
14
入出力部
11
第１記録領域
シリアル番号
12
第２記録領域
暗号化されたシリアル番号
13
第３記録領域

【図３】


START
S1
シリアル番号、
暗号化されたシリアル番号を
読み出す
S2
暗号化されたシリアル番号を
復号する
S3
読み出したシリアル番号と
復号したシリアル番号とを
比較する
S4
一致するか？
NO
YES
S5
正当な記録媒体である
S6
不当な記録媒体である
E N D

【図４】


100
105
コンテンツ DB
106
会員管理 DB
104
暗号鍵 DB
101
制御部
102
比較部
103
復号部
107
ネットワーク I/F
L
110
ネットワーク I/F
113
111
制御部
112
記録媒体 I/F
10

【書類名】　要約書

【要約】

【課題】　記録媒体の管理情報の改ざんを確実に検出するとともに、その正当性を確実に検証するための技術を提供する。

【手段】　管理情報を記録する第１記録領域と暗号化された前記管理情報を記録する第２記録領域とを有する記録媒体１０の正当性を検証する情報処理装置２０であって、前記記録媒体から前記管理番号および前記暗号化された管理番号を読み取るとともに、読み取った前記暗号化された管理番号の復号を制御する制御部（２４、２６）と、前記読み取った管理番号と前記復号された管理番号とが所定の対応関係にあるか否かを判定するとともに、その判定結果が肯定的なときに前記記録媒体が正当であると認定する比較部（２５）とを有する。

【選択図】　図２

出願人履歴情報

識別番号　〔３９５０１５３１９〕

１．変更年月日　１９９７年　３月３１日
［変更理由］　住所変更
住　所　東京都港区赤坂７－１－１
氏　名　株式会社ソニー・コンピュータエンタテインメント